STATE OF IDAHO

DEPARTMENT OF ADMINISTRATION

PREVENTING WORKPLACE VIOLENCE
A Guide for Agency Planners

DIRK KEMPTHORNE, GOVERNOR

Department of Administration
Pam Ahrens, Director

Division of Public Works, and
Office of Insurance Management
Ron Evans, Security Manager
rdevans@adm.state.id.us

650 W. State Street, Room 100
P.O. Box 83720
Boise, Idaho 83720-0079
(208) 332-1939
(208) 334-3818

http://www2.state.id.us/adm/pubworks/PreventingWorkplaceViolence

OCTOBER 2000

TABLE OF CONTENTS

PROGRAM DEVELOPMENT

I.   OVERVIEW

There are many different paths agencies can take in developing plans to prevent workplace violence. An approach that works well in one agency may not be suitable for another. This section outlines some broad guidelines that can help agencies in:

- Analyzing their current ability to handle potentially violent situations;
- Filling in any skill gaps that exist;
- Developing a procedure for employees to report incidents, and
- Developing response plans.

Intent: *This document is intended to be used as a guideline by state agencies. Nothing herein is intended to address all circumstances or workplace violence issues. The majority of materials are written for use by employees and agencies that encounter an internal threat or act of violence from another employee. If a threat or act of violence is received from an external source, the Idaho State Police and/or local law enforcement should be consulted as soon as possible. The State Security Manager can be of assistance with law enforcement liaison and security enhancements in your office.*

II.   FORMING A PLANNING GROUP

Successful agency programs usually start by forming a planning group. The planning group evaluates the agency's current ability to handle violent incidents and recommends ways to strengthen its response capability.

Typically, members of a planning group include representatives from Management, Human Resource (HR), Employee Assistance Program (EAP), Law Enforcement, and Security. Organizations that are too small to have a law enforcement/security component often have a representative of the local police on their planning group. Depending on the size and structure of the agency, membership may also include representatives from Safety, Public Relations, and other appropriate offices. The Department of Administration's State Security Manager is available to assist with agency planning activities and can facilitate liaison with law enforcement.

Participation on the planning group should **always** be offered to the agency's Deputy Attorney General. When this office is not represented on the planning group, it usually acts as consultants to it.

While many offices may be represented on the planning group, only a few of them will generally be involved in responding to reported incidents. For example, representatives from HR, EAP, and Security often make up the Incident Response Team (IRT). Typically, representatives from the other offices will not be involved in responding directly to incidents, but they will act as consultants to the IRT or play an active role only in certain types of situations. For the purposes

of this plan, the IRT is ordinarily comprised of representatives from HR, Security, Risk Management, Public Information Officer, a Deputy Attorney General, EAP representative and an on-site manager. It is not always necessary to involve all members of the Team in every incident requiring an IRT response.

III. STEPS IN THE PLANNING PROCESS

Analyze Agency's Current Ability To Handle Potentially Violent Situations

Conducting an analysis of the agency's current ability to handle potentially violent situations is a necessary effort. Looking at previous incidents that have occurred at your agency and evaluating how effectively they were handled is a good way to start. Attention should be given to identifying patterns of risk and potential prevention strategies, for example, where a particular workgroup is having a number of complaints in a given period of time.

Staff Expertise. Because of their different missions, agencies have different areas and levels of staff expertise. For example, some organizations have strong law enforcement capabilities, some have an in-house medical staff and some have criminal specialists. Agencies may have employees who have special skills that could be put to good use in a potentially violent situation, such as employees who are skilled in mediation, conflict resolution, crisis counseling, investigations, or threat assessment. Identifying offices and individuals ahead of time, working with them in the planning stages, and agreeing on a coordinated response effort is one of the most effective ways of preparing an agency to handle potentially violent situations should they arise. The State Security Manager can assist agencies in identifying these internal resources.

Level Of Security And Jurisdictional Issues. An important part of the analysis is to examine the current level of security at your agency. Follow the advice of your security office or, if you are in a building without a security staff, contact the State Security Manager or local law enforcement about recommended basic security measures.

Fill The Skill Gaps

Skill deficiencies exist even in large agencies with numerous resources at hand. In some organizations training is needed. However, crisis situations occur infrequently, and it is often not practical to maintain in-house expertise for every aspect of the agency's response plan.

If this is the case, suggested sources of outside assistance include:

Other Government Agencies. Get to know specialists in other government agencies. Federal agencies often share expertise, especially when crisis situations occur. They are also an invaluable source for learning about new training materials and effective training approaches.

Local Police. If you are not in a building served by Security officers, get to know your local police officers. Invite them in to work with your planning group. They can recommend security

measures, tell you about jurisdiction and what they would do if you called them during an incident. They can teach employees personal safety techniques and how to avoid becoming a victim.

Other Community Resources.   Locate and work with resources in your community. For example, if you don't have immediate access to emergency mental health consultation, you can work with your local community mental health department, "hotline" staff, hospital, or emergency crisis center. A nearby university may have faculties who are willing to be consulted.

Develop A Procedure For Employees To Report Incidents

The primary consideration in developing a reporting procedure is to make sure that it encourages employees to report all incidents, even minor ones. Some agencies use hotlines. Some arrange for a member of the team to take the calls, usually a specialist from Security. Other agencies require employees to report incidents to their supervisor (or to any agency supervisor), who in turn reports these incidents to Law Enforcement or Security.

Credibility for any reporting system will be dependent upon whether reports are handled quickly and effectively. Word spreads quickly among employees when a report is made and nothing is done, when a report is handled improperly, or when the allegations are not treated confidentially. Therefore, before a reporting procedure is announced to employees, ensure that the agency staff who will be responding to reported incidents are trained and able to handle any reported incidents.

> *Take threats seriously. Employees may not step forward with their concerns if they think that management will minimize these concerns.*

Also important to the success of any reporting system is management's encouragement for reporting incidents. Agency managers must create an environment that shows that management will always respond to reports of incidents and to employee concerns.

Incident reports should be reviewed on a periodic basis to provide feedback on the effectiveness of existing intervention strategies and prevention efforts.

Develop Plans To Respond To Workplace Violence Incidents

Given the wide range of incidents and situations that can occur at the work site (from disruptive behavior to shootings) and, within that range, the wide variation in threatening and disruptive behaviors, it is difficult for agencies to define specifically the responsibilities of the different offices that would be involved in responding to an incident under a workplace violence program.

Agencies have found it useful to classify incidents in broad categories, for example, emergency or non-emergency, emergency threats, bullying, disruptive behavior, or coworker/outsider.

Using these broad categories, agencies can determine which offices will generally respond to each type of incident and what role each office would play in the response effort. Agencies can plan for both immediate responses and long-term responses, when appropriate. For example, in the case of a suicide threat, the plan may state that the EAP counselor should recommend whether further action is appropriate. If the suicide threat seems imminent, the plan may state that the community's emergency services (or local police) are contacted. The plan would also state what management would do if the EAP counselor were not immediately available.

It will become apparent that plans for a coordinated response to reported incidents must be kept flexible. Responsibility for overall coordination and direction is usually assigned to one individual or one office. The coordinator must have the flexibility to use the plan as a guideline, not a mandatory set of procedures. More important, the coordinator must have the flexibility to tailor the recommended response to the particular situation. It is important to recognize that threatening situations often require creative responses. Given this, the importance of flexibility cannot be overemphasized.

> *You can't always prevent violence because violent incidents are often unpredictable, but you can reduce the risk by planning ahead and being prepared to act swiftly to deal with threats, intimidation, and other disruptive behavior at an early stage.*

Experts stress the need for backup plans in situations calling for an immediate response where the individual responsible for a certain aspect of the response effort has gone home for the day, is on vacation, or is otherwise unavailable. Taking a team approach in responding to a potentially violent situation is an ideal way to provide backup coverage. A team approach ensures that all staff in HR, the EAP, Security, and other offices are thoroughly trained and prepared to work together with management to deal with potentially violent situations. It ensures coverage, regardless of which person in each of the offices is on duty when the incident occurs.

DEVELOPMENT OF WRITTEN POLICY STATEMENT

I. OVERVIEW

This section outlines advantages, methods, and warnings while putting together your written policy, including:

- Advantages;
- Policy contents;
- Recommended approaches;
- The use of definitions;
- Zero tolerance issues;
- Investigation issues; and
- Addressing computer security in the written policy statement.

II. ADVANTAGES OF WRITTEN POLICIES

Once a workplace violence program is ready to be implemented, agencies must decide whether to issue a written policy statement. Among the advantages of issuing a statement are:

- It informs employees that the violence policy covers intimidation, harassment, and other inappropriate behavior that threatens or frightens them;
- It encourages employees to report incidents;
- It informs employees whom to call; and
- It demonstrates senior management's commitment to dealing with reported incidents.

Agencies are strongly encouraged to implement a written policy statement, however programs can be implemented without such. In these agencies, employees are often given information about the program (especially whom to call) in training sessions, on posters, in newsletter articles, or by other similar methods. Note: Agencies have an inherent right to take action against employees who engage in disruptive or threatening behavior whether or not they have issued a written policy statement.

III. POLICY STATEMENT CONTENTS

A workplace violence policy statement should convey that:

- All employees are responsible for maintaining a safe work environment;
- The policy covers not only acts of physical violence, but harassment, intimidation, and other disruptive behavior;
- The policy covers incidents involving coworkers and individuals from outside the agency perpetrating violence against agency employees;
- The agency will respond appropriately to all reported incidents;

- The agency will act to stop inappropriate behavior; and
- Supervisors and all of the offices involved in responding to incidents will be supported by agency management in their efforts to deal with violent and potentially violent situations.

IV.   RECOMMENDED APPROACHES

Consider the following recommendations in developing your written policy statement:

Keep It Brief

A Written Policy Statement Should Be Brief And Simple. Implementation details can be provided in training and in more detailed backup documents. For example, roles and responsibilities of the various individuals involved in responding to potentially dangerous situations can be outlined in memoranda of understanding, in operating manuals or instructions rather than in the written policy statement that is issued to all agency employees. This approach gives agency staff the flexibility they will need to deal creatively with these fluid, unpredictable situations.

Consider The Disadvantages Of Using Definitions

There Are Disadvantages To Using Definitions Of Terms Such As Violence, Threats, And Harassment In Your Written Policy Statement. Definitions can discourage employees from reporting incidents that they do not believe fall within the definition. The reporting system should not deter employees from reporting situations that frighten them. An employee knows a threat or intimidation or other disruptive behavior when he or she experiences it. Definitions are not necessary. However, if you want to clarify the scope of your organization's concept of one or more of the terms in the policy, you could use examples, such as verbal and non-verbal intimidating behavior.

Another consideration is that definitions are often restrictive and may create legal problems in the future when disciplinary actions are initiated against the perpetrators of workplace violence. Use of definitions can make a case more difficult to defend on appeal.

Be Cautious With "Zero Tolerance"

Consider That There Could Be Negative Consequences From Using The Term "Zero Tolerance". It could create legal problems in the future when disciplinary actions against the perpetrators of workplace violence are implemented. Use of the term could make it more difficult to defend a case on appeal because a third party could conclude, however mistakenly and inappropriately, that the agency has not considered a penalty appropriate for the particular offense.

There are other possible consequences. The term "zero tolerance" might appear to eliminate any flexibility an agency has in dealing with difficult situations even if this is not intended. Another

undesirable side effect is that the appearance of inflexibility may discourage employees from reporting incidents because they do not want to get a coworker fired; but just want the behavior stopped. This appearance of inflexibility also may discourage early intervention in potentially violent situations.

V.   INVESTIGATION ISSUES FOR THE AGENCY PLANNING GROUP

Additional fact finding/investigating issues that the agency-planning group should address:

- Agency policy should be formulated ahead of time regarding such matters as no- shows, whether to allow tape recording of the interviews, and whether to allow the presence of additional persons during the interviews. Policy should be based on sound legal analysis.
- Keep in mind that the routine, administrative details can't be ignored. Prior to beginning the actual investigation, the manager should be given all administrative details, i.e., who gets the report and whom to contact regarding other administrative matters, such as the manager's pay, parking, and overtime. Smaller agencies may wish to utilize the availability of the State Security Manager to assist with many of these important details.
- Consider giving the manager a list of factors considered in making credibility determinations. They are:
  - The witness's opportunity and capacity to observe the event or act in question;
  - The witness's character;
  - Any prior inconsistent statement by the witness;
  - The witness's bias, or lack of bias;
  - The contradiction of the witness's version of events by other evidence or its consistency with other evidence;
  - The inherent improbability of the witness's version of events; and
  - The witness's demeanor.
- Every step of the investigation should be objective, impartial, and unbiased.
- The investigative report will contain:
  - Statements of witnesses; and
  - Documentary evidence.
- The investigative report generally does not include an analysis of the report.
  - Both the manager and the person who prepares the analysis of the report should be objective, impartial, and unbiased.
  - Consider developing a letter signed by the agency head or high-level designated official authorizing the investigation and requiring employees to cooperate. (See, however, the information below regarding warnings to the subjects of administrative investigations when it is necessary to require cooperation.)
  - Ensure that all appropriate agency personnel are aware of the requirements discussed above regarding warnings when compelling statements from the subject of an administrative investigation.

VI.   COMPUTER SECURITY

Agency planning groups should address ways to safeguard computer systems. There have been cases where employees have sabotaged computer equipment, computer systems, and computer records. Therefore, whenever a threat of sabotage is suspected, procedures should be initiated to prevent the person from having access to the facility's computer system.

It is important to act quickly whenever there is reason to believe that an employee or ex-employee may commit such an act. It is standard practice to collect identification, building passes, keys, and parking passes when employees leave their jobs. Often, however, no one thinks to block access to computer systems or networks.

Some agencies, when terminating employees, bar them from the premises and eradicate their passwords to computer systems that are accessible from outside the premises.

This type of access information is sometimes difficult to determine; often, it is not readily available in one central place. For example, information technology administrators may know who has access to various computer systems, and the facilities manager may know who has access to the computer systems that control the building's heating, air-conditioning, and other support functions for the facility. The agency-planning group, as part of the response plan, should talk to the information/computer security officer or computer system administrators to determine the vulnerability of the computer networks and the procedures that need to be implemented to lock individuals out of these systems. It is suggested that agencies establish and maintain a checklist of network access granted to each employee.

Consult With Legal Counsel

Consult your Deputy Attorney General for the legal implications of your draft policy.

Other Considerations for the Agency and Investigator. Consider developing a letter signed by the agency head or high-level designated official authorizing the investigation and requesting employees' cooperation.

INCIDENT RESPONSE TEAM

I.   OVERVIEW

This section will focus on the critical necessity of an IRT who will address:

- Prevention of violent situations;
- Response Team training for employees and supervisors;
- Screening new hires;
- Maintaining a secure workplace; and
- Alternative dispute resolution.

II.   PREVENTION

One major component of any workplace violence program is prevention. The topics in the previous sections, such as program development, are important parts of a workplace violence prevention program. This section will focus on **additional** measures that can be taken to reduce the risk of violent behavior.

III.   WARNING SIGNS OF VIOLENCE

The first question many people ask when starting to develop a workplace violence prevention program is, "*How can we identify potentially violent individuals?*" It is understandable that people want to know this. "Early warning signs" and "profiles" of potentially violent employees are in much of the literature on the subject of workplace violence. It would save time and solve problems if managers could figure out ahead of time what behaviors and personality traits are predictive of future violent actions.

Indicators Of Potentially Violent Behavior

No one can predict human behavior and there is no "specific profile" of a potentially dangerous individual. However, indicators of increased risk of violent behavior are available. These indicators have been identified by the Federal Bureau of Investigation's National Center for the Analysis of Violent Crime, Profiling and Behavioral Assessment Unit in its analysis of past incidents of workplace violence. These are some of the indicators:

- Direct or veiled threats of harm;
- Intimidating, belligerent, harassing, bullying, or other inappropriate and aggressive behavior;
- Numerous conflicts with supervisors and other employees;
- Bringing a weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to guns, or fascination with weapons;

- Statements showing fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a problem, or statements indicating identification with perpetrators of workplace homicides;
- Statements indicating desperation (family, financial, and other personal problems) to the point of contemplating suicide;
- Drug/alcohol abuse; and/or
- Extreme changes in behaviors.

Each of these behaviors is a clear sign that something is wrong. **None should be ignored.** By identifying the problem and dealing with it appropriately, managers may be able to prevent violence from happening. Agency planning groups should ensure that the appropriate staff member (or an IRT) is prepared to assist supervisors and other employees in dealing with such situations. Some behaviors require immediate police or security involvement, others constitute actionable misconduct and require disciplinary action, or others may indicate an immediate need for an EAP referral.

On the other hand, it is seldom (if ever) advisable to rely extensively on what are inappropriately referred to as "profiles" or "early warning signs" to predict violent behavior. "Profiles" often suggest that people with certain characteristics, such as "loners" and "men in their forties", are potentially violent. This kind of categorization will not help predict violence, and it can lead to unfair and destructive stereotyping of employees.

The same can be said of reliance on "early warning signs" that include descriptions of problem situations, such as "in therapy", "has had a death in the family", "suffers from mental illness," or "facing a reduction in force (RIF)". Everyone experiences stress, loss, or illness at some point in life. All but a very few people weather these storms without resorting to violence. Managers should, of course, be trained to deal with the kinds of difficulties mentioned here, such as bereavement or mental illness. However, this training should focus on supporting the employee in the workplace, and not in the context of, or on the potential for, workplace violence.

IV.   TRAINING

Training is a critical component of any prevention strategy. Training is necessary for employees, supervisors, and the staff members of each office that may be involved in responding to an incident of workplace violence. Training sessions conducted by the agency's EAP, Security, and HR staffs are particularly helpful, enabling employees to become acquainted with experts within the agency who can help them when potentially violent situations arise. Employees and supervisors seek assistance at a much earlier stage when they personally know the agency officials who can help them.

> ***Providing appropriate training informs employees that management will take threats seriously, encourages employees to report incidents, and demonstrates management's commitment to deal with reported incidents.***

Employee Training

All employees should know how to report incidents of violent, intimidating, threatening, and other disruptive behavior. All employees should also be provided with phone numbers for quick reference during a crisis or an emergency. In addition, workplace violence prevention training for employees may also include topics such as:

- Explanation of the agency's workplace violence policy;
- Encouragement to report incidents;
- Ways of preventing or diffusing volatile situations or aggressive behavior;
- How to deal with hostile persons;
- Managing anger;
- Techniques and skills to resolve conflicts;
- Stress management, relaxation techniques, wellness training;
- Security procedures, i.e., the location and operation of safety devices such as alarm systems and call boxes;
- Personal security measures; and
- Programs operating within the agency that can assist employees in resolving conflict, i.e., the EAP, mediation counselors, etc.

Supervisory Training

In addition to the training suggested above, special attention should be paid to general supervisory training. The same approaches that create a healthy, productive workplace can also help prevent potentially violent situations. It is important that supervisory training include basic leadership skills, such as setting clear standards, addressing employee problems promptly, and using the probationary period, performance counseling, discipline, and other management tools conscientiously. These interventions can keep difficult situations from turning into major problems. Supervisors don't need to be experts on violent behavior; what is needed is a willingness to seek advice from the experts.

Some agencies include training on workplace violence as part of general supervisory training, some conduct separate training sessions on workplace violence, and some include it in crisis management training. Whichever approach is taken, supervisory training should cover:

- Ways to encourage employees to report incidents in which they feel threatened for any reason by anyone inside or outside the organization;
- Skills in behaving compassionately and with support towards employees who report incidents;
- Skills in taking disciplinary actions;
- Basic skills in handling crisis situations;
- Basic emergency procedures; and
- How to ensure that appropriate screening of pre-employment references has been done.

Incident Response Team Training

The members of the IRT need to be competent in their own professions, **and** they need to know when to call for outside resources. Participating in programs and training sessions sponsored by government and professional organizations, reading professional journals and other relevant literature, and networking with others in their profession are all helpful in dealing with workplace violence situations.

Team members also need to understand enough about each other's professions to allow them to work together effectively. Response team training should allow discussion of policies, legal constraints, technical vocabulary, and other considerations that each profession brings to the interdisciplinary group.

Much of the IRT training can be accomplished by practicing responses to different scenarios of workplace violence. Practice exercises can help the staff understand each other's responses to various situations so there is no confusion or misunderstanding during an actual incident. In addition, practice exercises can prepare the staff to conduct the supervisory training suggested above.

The team members also need to consult regularly with other personnel within the organization who may be involved in dealing with potentially violent situations. Those who are consulted on an *ad hoc* basis should receive appropriate training as well.

V. PRE-EMPLOYMENT SCREENING

Pre-employment screening is an important part of workplace violence prevention. Prior to hiring an employee, the agency should always check with its servicing personnel office and legal office, if necessary, to determine what pre-employment screening techniques (such as interview questions, background and reference checks, and drug testing) are appropriate for the position under consideration and are consistent with federal and state laws and regulations. Pre-employment screening is one of the most effective measures utilized to reduce workplace violence incidents.

VI. SECURITY MEASURES

Maintaining a physically safe work place is part of any good prevention program. Agency facilities use a variety of security measures to help ensure safety. These include:

- Employee photo identification badges;
- On-site security services and/or individually coded card keys for access to buildings and areas within buildings according to individual needs; and
- Security force assistance in registering, badging, and directing visitors in larger facilities.

VII. USING ALTERNATIVE DISPUTE RESOLUTION (ADR) AS A PREVENTIVE STRATEGY

Some agencies use ombudsman programs, facilitation, mediation, and other methods of alternative dispute resolution (ADR) as preventive strategies in their workplace violence programs. ADR approaches often involve a neutral third party that can assist disputing parties resolve disagreements. ADR is most helpful in workplace violence programs at the point when a problem first surfaces, i.e., before an employee's conduct rises to a level that warrants a disciplinary action.

FACT FINDING AND INVESTIGATING

I.   OVERVIEW

This section will focus on an agencies response to a threat of violence and the actions taken after a violent incident.   The investigation, which follows a threat or violent act, must be acted on quickly and proceed with respect to confidentiality and legal issues. There are several methods of investigation including:

- Threat assessment;
- Resources;
- Purpose of a threat assessment program;
- Identification of the perpetrator;
- Assessing the risks;
- Interviewing; and
- Case management.

II.   THREAT ASSESSMENT

Introduction

Employees who feel threatened want to know what the agency is doing to protect them and what measures they should take to protect themselves. Since it is impossible to know with any certainty whether a threat is going to be carried out, the agency should always respond to threats in a serious manner and act as though the person may carry out the threat.

This section will provide a basic understanding of the threat assessment process. It gives background information for personnel who may be involved in the process, but does **not provide instructions on threat assessment techniques.**

Threat Assessment Assistance

A supervisor can handle many cases involving threatening behavior expeditiously and effectively with the assistance of one or more members of the agency's IRT. The security or law enforcement representative on the agency's team will ordinarily assess risks, often in consultation with the EAP and HR staff, and make recommendations for appropriate strategies and security measures to protect employees. However, in case a situation requires more expertise than team members can ordinarily provide, it may be helpful for the agency's planning group to identify experts in threat assessment ahead of time.

If an agency elects to request assistance from local law enforcement, due to the urgency of the situation, the nearest State Police office should also be notified. State Police officials will provide assistance to local law enforcement and may have greater resources available. The State

Security Manager should also be notified to determine if an immediate increased security presence is warranted and to provide liaison between the victim agency and law enforcement if necessary.

Gathering Information

It is also a good idea to work out ahead of time which team member will gather which types of information concerning an individual who makes a threat. Multiple sources of information need to be consulted to better understand the person's behavior (also see VII. Assessing The Risks).

In some cases, the agency's IRT can collect current and reliable information (which would include an investigative report) and then consult with a threat assessment professional to develop options for managing the situation. In other cases, the agency's IRT uses a threat assessment professional to conduct the initial investigation, assess the risks, and make recommendations for managing the situation.

Threat assessment investigations differ from criminal or administrative investigations in that the purpose of the threat assessment investigation is to provide guidance on managing the situation in a way that protects the employees.

III.   THREAT ASSESSMENT RESOURCES

Threat assessment is an evolving technical field. It is important to find a qualified professional to assist you if the need arises. A few state agencies have experience with threat assessment professionals within their organizations; some have threat management units within their criminal investigative services.

IV.   FUNDAMENTAL PRINCIPLES OF THREAT ASSESSMENT

Notwithstanding the growing importance of threat assessment for law enforcement and security professionals, systematic thinking and guidance in this area has been lacking in many organizations. Some law enforcement and security communities currently do not have clearly articulated processes or procedures to steer their actions when they are made aware of threat-of-violence subjects and situations. Without guidelines for making threat assessments, otherwise competent law enforcement professionals may be less thoughtful and thorough than they might be in handling such incidents. To fill the void, the following presents four fundamental principles that underlie threat assessment investigation and management. A model and process for conducting comprehensive threat assessment investigations follow them.

- Violence is a process, as well as an act. Violent behavior does not occur in a vacuum. Careful analysis of violent incidents shows that violent acts often are the culmination of long-developing, identifiable trails of problems, conflicts, disputes, and failures.
- Violence is the product of an interaction among three factors: (i) the individual who takes violent action; (ii) stimulus or triggering conditions that lead the subject to see violence as

an option, "way out", or solution to problems or life situation; and (iii) a setting that facilitates or permits the violence, or at least does not stop it from occurring.

- A key to investigation and resolution of threat assessment cases is identification of the subject's "attack-related" behaviors. Perpetrators of targeted acts of violence engage in discrete behaviors that precede and are linked to their attacks; they consider, plan, and prepare before engaging in violent actions.

- Threatening situations are more likely to be successfully investigated and managed if other agencies and systems, both within and outside law enforcement or security organizations, are recognized and used to help solve problems presented by a given case. Examples of such systems are those employed by prosecutors, courts, probation, corrections, social service and mental health agencies, employee assistance programs, victim's assistance programs, and community groups.

V. FUNCTIONS OF A THREAT ASSESSMENT PROGRAM

The three major functions of a threat assessment program are:

- Identification of a potential perpetrator;
- Assessment of the risks of violence posed by a given perpetrator at a given time; and
- Management of both the subject and the risks that he or she presents to a given target.

VI. IDENTIFYING THE PERPETRATOR

Before taking any action involving a potential perpetrator, **consult your agency's Deputy Attorney General** in order to avoid any breaches in confidentiality or violations of constitutional rights. Should you determine that the perpetrator is not a state employee, immediately notify the Idaho State Police and local law enforcement authorities.

The process of identifying a potential perpetrator involves:

- Defining criteria that could lead to a person becoming a subject of a threat assessment investigation;
- Determining the areas within the law enforcement or security organization that will be responsible for receiving information about possible subjects and conducting threat assessment investigations;
- Notifying those individuals and organizations that might come in contact with -- or know of -- potential subjects about the existence of a threat assessment program; and
- Educating notified individuals and organizations about the criteria for bringing a concern about potential violence to the attention of managers.

VII.   ASSESSING THE RISKS

The second goal of a threat assessment program is to evaluate the risks a person under suspicion may pose to particular targets. Risk assessment involves two primary functions: investigation and evaluation.

Investigation

The primary objective of a risk assessment investigation is to gather information on a subject and on potential targets. **Before gathering information to be used in this investigation, consult with the Deputy Attorney General to determine confidentiality requirements and/or other legal issues and concerns.** Multiple sources of information should be consulted to learn about a subject's behavior, interests, and state of mind at various points in time:

- Determine if the threat source is a state employee. If not, consult with law enforcement on an appropriate course of action. If in doubt, call the State Security Manager.
- If the threat source is a state employee, consult with agency Deputy Attorney General and State Security Manager for assistance and course of action.
- Personal interviews with the subject.
- Material created or possessed by the subject, including journals and letters, and materials collected by the subject, such as books and magazines, that may relate to the investigation.
- Persons who know or have known the subject, including family members, friends, coworkers, supervisors, neighbors, landlords, law enforcement officers, social service or mental health staff, and previous victims of unacceptable behavior (including violence) committed by the subject.
- Record or archival information, including police, court, probation, and correctional records; mental health and social service records; and notes made by those aware of the subject's interest in a particular target, such as security personnel, managers, victims, or colleagues.

Information About The Subject

At the beginning of a threat assessment investigation, it is important to secure detailed descriptions of the subject's behaviors and actions that prompted other persons to notice the subject. The types of information useful for threat assessment include data about overwhelmingly or unbearably stressful experiences, and the subject's ability to cope at such times. Behavioral data about the subject's motives, intentions, and capacities is critical; of particular importance is information about attack-related behaviors:

- The subject has expressed interest in possible targets, including particular, identifiable targets;
- The subject has communicated with or about potential targets;
- The subject has considered and/or attempted to harm self or others;

- The subject has secured or practiced with weapons; and/or
- The subject has followed or approached potential targets, either with or without weapons, at events or occasions.

Interviewing The Subject

Whether to interview the subject of a threat assessment investigation can be a key question; the decision depends on several factors:

- The manager's need for information;
- The facts leading to initiation of investigation;
- The manager's legal standing in relation to the subject;
- The resources available to the manager;
- The manager's training and experience in interviewing;
- The stage of the investigation; and
- The manager's strategy for resolving the case.

A decision to interview a subject should be made on the basis of case facts. Generally when there has been face-to-face contact between subject and target or the subject has communicated a threat to the target, an interview is a good idea. An interview under such circumstances may have several goals. It may signal that the subject's behavior has been noticed, permit the subject's story to be related to a third party, gather information that is the basis for corroboration, and provide an opportunity for communicating that the subject's behavior is unwelcome, unacceptable, and must cease.

Any interview is a vehicle for gathering information about the subject that can be used to assess the threat that a subject poses and to manage that threat. Therefore, threat assessment interviews are most productive if they are conducted respectfully and professionally. The task of the manager is twofold: (i) to gather information about the subject's thinking, behavior patterns, and activities regarding the target(s), and (ii) to encourage change in the subject's behavior. By showing an interest in the subject's life that is neither unduly friendly nor harsh, a manager can increase the likelihood of the interview's success.

In some cases, however, an interview may intensify the subject's interest in the target or increase the risk of lethal behavior. For example, a desperate and suicidal subject, self-perceived as having been abandoned, who has been stalking a former partner, may sense that time is running out and be prompted by an interview to engage in more extreme behavior before "they put me away". In such a circumstance, the manager may need to expend additional resources, perhaps increasing security for the target, arranging hospitalization or arrest of the subject, or monitoring or surveillance of the subject. Subject interviews, therefore, should be considered and conducted within the context of overall investigative strategy.

Information About The Target

A man who, over days and weeks, has been following a secretary whom he met once but with whom he has no relationship, appears to have picked out a potential target. An employee, fired by a manager whom he blames for discriminating against him and causing the breakup of his family, has told former coworkers that he will "get even". Once again, a potential target appears to have been selected. To prevent violence, the threat assessment manager requires information on the targeted individual. Relevant questions about the target might include the following:

- Are potential targets identifiable, or does it appear that the subject, if considering violence, has not yet selected targets for possible attack?
- Does the subject know the potential target well? Is the subject acquainted with a targeted individual's work and personal lifestyle, patterns of living, daily comings and goings?
- Is the potential target vulnerable to an attack? Does the targeted individual have the resources to arrange for physical security? What might change in the target's lifestyle or living arrangements that could make attack by the subject more difficult or less likely, i.e., is the targeted individual planning to move, spend more time at home, or take a new job?
- Is the target afraid of the subject? Is the targeted individual's degree of fear shared by family, friends, and/or colleagues?
- How sophisticated or naive is the targeted individual about the need for caution? How able is the individual to communicate a clear and consistent *I want no contact with you* message to the subject?

Evaluation

A two-stage process is suggested to evaluate information gathered about the subject and the potential target(s). In the first stage, information is evaluated for evidence of conditions and behaviors that would be consistent with an attack. The second stage of evaluation seeks to determine whether the subject appears to be moving toward or away from an attack. After analyzing the available data, the threat assessor is left with these questions:

- Does it appear more or less likely that violent action will be directed by the subject against the target(s)? What specific information and reasoning lead to this conclusion?
- How close is the subject to attempting an attack? What thresholds, if any, have been crossed (i.e., has the subject violated court orders, made a will, given away personal items, expressed willingness to die or to be incarcerated)?
- What might change in the subject's life to increase or decrease the risk of violence?
- What might change in the target's situation to increase or decrease the risk of violence?

VIII. CASE MANAGEMENT

The first component of threat assessment case management involves developing a plan that moves the subject away from regarding violence against the target as a viable option. Such a plan

is likely to draw on resources (personnel and facilities) from systems within the threat assessment unit's parent organization, as well as those outside the agency. The second component is plan implementation. The best developed and supported case management plan will be of little use in preventing violence if the plan is not implemented and monitored. The plan must remain flexible to accommodate changes in the subject's life and circumstances. The final management component is formal closing of the case.

Case Management Development

Once an evaluator determines that a given subject presents a risk of violence to a targeted individual, the next task is to develop a plan to manage the subject and the risk. The evaluator then proceeds to identify those internal and external systems that may be helpful in managing the problems presented by the subject. In certain situations, such as those in which the subject has been stalking an identifiable target in a jurisdiction that has an enforceable and effective anti-stalking law, the best way to prevent violence and minimize harm to the targeted individual may be to prosecute the case vigorously.

A good relationship between threat assessment managers and prosecutors can influence the priority assigned to the case and the extent to which prosecutorial and judicial processes facilitate its resolution. Such relationships also may affect the court's disposition of the case, including sentencing of a convicted offender.

Even conviction and imprisonment, however, do not guarantee that the target will be safe from the subject. If the subject has been unable or unwilling to let go of the idea of a relationship with the target, or if the subject attributes the pains and misfortunes of his or her life to the targeted individual, it may make sense to consider strategies by which the subject is encouraged to change the direction, or intensity, of his interest. A subject engaged in activities that bring success and satisfaction is less likely to remain preoccupied with a failed relationship. Family, friends, neighbors, or associates may play a role in suggesting and supporting changes in the subject's thinking and behavior. In addition, mental health (EAP) and social service staff may be of great assistance in aiding the subject to formulate more appropriate goals and develop skills and strengths that are likely to result in life successes.

At least one aspect of a case management plan concerns the target. If the subject is to be prohibited from contact with the target, the target needs to understand what to do (i.e., whom to call and how to contact the official handling the case) if the subject initiates direct or indirect contact.

Case Management Implementation

The most carefully crafted plan will have little effect if it remains in the manager's files and is not translated into action. Although no procedures or techniques can guarantee that a subject of comprehensive threat assessment will not attempt violent action toward a target, two activities are known to help reduce the risk of violence, and, in the instance of a bad outcome, assist the threat assessment team in any post-incident review.

First, documentation of data and reasoning at every stage of a threat assessment investigation is essential. Undocumented or poorly documented information gathering and analysis are suspect in and of themselves, and they provide little foundation for review or for efforts to learn from, and improve on, experience. Without clear documentation, managers are left with only their recollections, which can be both partial and faulty and are subject to criticism as retrospective reconstruction. A carefully and comprehensively documented record may be criticized for imperfect data-gathering or flawed analysis, but such a record also demonstrates both thoughtfulness and good faith, critical questions in any post-incident review.

Second, consultation at every major stage of the threat assessment process can be a significant case management tool. Consultants may be members of the threat assessment unit or external experts. To be effective, a consultant should be knowledgeable in areas relevant to the case and be known and trusted by the managers. For example, in a case where a subject has a history of diagnosed mental disorders and the primary manager is unfamiliar with mental health language and concepts used in the records, an expert in psychology or psychiatry can provide invaluable insight and advice.

In addition to providing special expertise, consultants may notice and ask about questions in a case that remain to be explored or answered. Even proficient managers are occasionally vulnerable to "missing the forest for the trees". A consultant, such as a fellow threat assessment specialist who has not been involved with the case, may offer a comment that can redirect or sharpen an ongoing investigation.

In the event of a bad outcome, use and documentation of consultant expertise may demonstrate that the threat assessment team sought additional perspectives and ideas and did not get stuck with "tunnel vision".

Closing The Case

The final task of threat assessment case management is closing the case. When a threat assessor determines that the subject has moved far enough away from possible violent action toward the target to no longer cause appreciable concern, the case can be considered for closing. At this time, it may be important to ask:

- What has changed in the subject's life that appears to lessen the likelihood that the subject is interested in or will attempt violent action toward the target?
- Which components of the case management plan seemed to affect the subject's thinking or capacity to initiate violent action, and to what extent?
- What life circumstances might occur that would again put the subject at increased risk of contemplating, planning, or attempting violent action toward the original target or other potential targets?
- Are there supports in place (or that can be developed) that will be known and available to the subject at a future time when the subject is again at risk of moving toward violent behavior?

While social commentators and analysts may debate the myriad reasons that lead to growing national concern about targeted violence, law enforcement and security organizations are increasingly being called upon to examine individual situations and make judgments and determinations about the risks of violence that one person might present to an identifiable target. In cases related to stalking behaviors, workplace violence, attacks on public officials and figures, and other situations where targeted violence is a possibility, comprehensive and carefully conducted threat assessment investigations can safeguard potential targets, deter potential attackers, and serve the public.

> *The information which follows, provides guidance for the agency-planning group. It is not technical information for professional managers; nor is it a summary of fact- finding or investigating procedures. Rather, it is intended to provide the agency- planning group with a general overview of fact-finding/investigating considerations. It is also important to note that this section discusses investigations that are administrative inquiries that are distinct from criminal investigations.*

IX.   RECEIVING A COMPLAINT

I Can't Work Here Anymore. I'm Afraid He May Actually Kill One Of Us.

The supervisor hears the details of the incident that is causing the employee to feel threatened. Now the supervisor has to do something. The incident can't be ignored. It must be reported. Once reported, the members of the IRT (along with the supervisor) have to look into it.

What You Need To Know.

As in all other serious administrative matters that come to the agency's attention, more must be discovered about what is going on in this situation. You want to know:

- **What** happened?
- **Who** was involved?
- **Where** it happened?
- **When** it happened?
- **Why** it happened?
- **How** it happened?

What To Do Next

Sometimes taking a few minutes for a cursory overview will give you enough information to know what to do next. Of course, if there is imminent danger, law enforcement must be notified immediately.

However, if there is no imminent danger, deciding what to do next will depend on agency procedures and the strategy/relationship you have worked out ahead of time with your agency's Deputy Attorney General, and the law enforcement or security organization that has jurisdiction over your work site.

X.   TYPES OF INVESTIGATIONS

Often, one of the first decisions to be made is whether to conduct an administrative or a criminal investigation. The answer will depend on whether the facts as presented indicate possible criminal behavior. Since arriving at a decision generally involves discussion with law enforcement personnel, the Deputy Attorney General and HR specialists, it is imperative to coordinate efforts fully with these offices ahead of time. Also, as discussed below, an important point of these discussions is to ensure that actions taken by an agency during an administrative investigation do not impede potential criminal prosecutions.

XI.   ADMINISTRATIVE INVESTIGATIONS

Use Qualified Personnel

If a decision is made to conduct an administrative investigation, **it is important to use a qualified and experienced individual or team who will normally work closely with the agency Deputy Attorney General**. The agency-planning group should locate one or more such individuals or team members before the need arises. Your agency probably already has qualified personnel, for example, in the Office of the Attorney General. Some other good places to look in your own agency are HR and Security. In some agencies, these offices have their own managers. In others, they contract with private managers, or utilize the services of managers from the Idaho State Police. In any case, they should be able to help you locate trained, qualified personnel ahead of time.

It is important to use an investigator who conducts the inquiry in a fair and objective manner. The investigation should be conducive to developing truthful responses to issues that may surface. It must be conducted with full appreciation for the legal considerations that protect individual privacy. It is imperative that an atmosphere of candor and propriety be maintained.

Ensure That Criminal Prosecutions Are Not Compromised

Criminal prosecutions must not be compromised by actions taken during administrative investigations. It is necessary to ensure that the administrative manager, management, and all

members of an IRT understand that actions taken during an administrative investigation may compromise potential criminal prosecutions. If the agency obtains statements from the subject of the investigation in the wrong way, the statements can impede or even destroy the ability to criminally prosecute the case. On the other hand, if handled correctly, statements made in administrative investigations could prove vital in subsequent criminal proceedings.

Therefore, in a case where a decision is made to conduct an administrative investigation and there is potential criminal liability, it is good practice to give the **subject** of the investigation what are usually called "non-custodial warnings and assurances". That is, the person is given the **option** of participating in the interview after being warned that any statements he or she makes **may** be used against him or her in criminal proceedings. The option not to participate in the interview is exercised by the person's invocation of his or her Fifth Amendment right against self- incrimination. Note: Since the person is not legally in custody, he or she is not entitled to an attorney, but use of any attorney should not be discouraged.

If a decision is made to **compel** the subject of an investigation to participate in an interview (instead of being given an option to participate), the investigator should give *Garrity* (Garrity v. State of New Jersey, 385 US 493 [1967]) warnings. This means that the person is told that statements he or she makes (and the information gained as a result of these statements) **cannot** be used against him or her in criminal proceedings.

Even if an investigator does not actually give *Garrity* warnings, if the investigator compels the subject to give a statement, the information in the statement **(and the information gained as a result of the statement)** <u>usually</u> **cannot** be used in criminal proceedings.

Since this may make criminal prosecution impossible, an investigator should never give *Garrity* **warnings or compel statements from the subject of an investigation without the permission of the appropriate Deputy Attorney General or prosecutor's office.** The agency's Deputy Attorney General usually obtains such permission. Since this is an extremely complicated consideration, be sure to work closely with the Office of Attorney General and law enforcement organization. In potentially violent situations, it is often difficult to determine whether the misconduct is a criminal offense. **When there is any doubt, check it out first.**

XI.   PREPARATION AND PROCEDURES IN ADMINISTRATIVE INVESTIGATIONS

A thorough and professional investigative product is the result of thorough, professional preparation and procedures. Personally obtaining information from individuals will constitute a significant part of any investigation. An awareness of the skills and techniques necessary for effective interviewing is required.

In preparing for and conducting investigations, experienced professional investigators have found the following approaches to be effective.

Reviewing Available Information

The investigator, after thoroughly reviewing the information that gave rise to the investigation, is ready to begin the investigation process. Discrepancies or deficiencies in the information should be noted so they can be addressed during the interviews.

Selecting An Interview Site

Since the investigator is conducting an official investigation, he or she should conduct as many interviews as possible in an official environment, i.e., in government workspace and not in restaurants, cars, or private homes. Privacy is the most important consideration in selection of an interview site. The investigator should guarantee that the room will be available for the entire interview, so there is no disruption of the interview once it begins. The interview room should be comfortably furnished with as few distractions as possible.

Scheduling The Interview

Depending on the circumstances of the situation, the investigator may or may not want to contact the individual in advance. In either event, the investigator should advise the individual of the general nature and purpose of the interview. If the individual declines the interview, the investigator should attempt to dissuade the individual and, if unsuccessful, ascertain and record the reasons for the declination. If the individual fails to appear more than once for the interview, the investigator should follow whatever policy has been decided upon by the agency ahead of time.

Allowing The Presence Of Additional Persons

There may be instances when the investigator or the individual being interviewed wishes to have an additional person present. Investigators sometimes prefer to have an agency representative present when interviewing the subject of the investigation. In any event, the investigator should follow whatever policy has been decided upon by the agency ahead of time.

Taking Notes

Since watching an investigator take notes may be intimidating to some people, it is important to establish rapport before beginning to take notes. The investigator should concentrate on observing the individual during the interview. Taking notes should not unduly interfere with observation. Note materials should be positioned inconspicuously and not become a focus of attention. The investigator should learn and exercise the skill of taking adequate notes while still observing the individual and without distracting the person being interviewed. In some cases, it may even be useful to have a second investigator or other official present to record the written material.

Should taking notes have a materially adverse effect on the interview process, the investigator may explain the purpose of recording the notes. The notes are intended for the investigator's use in preparing a report and are not a verbatim transcript of the interview. The investigator can modify or cease recording so long as the information can be documented in adequate detail after the interview.

Maintaining Control Of The Interview

Questions developed ahead of time can be memorized, but they should never be read verbatim from a list or recited in a perfunctory manner. The investigator should know in advance the topics of concern to be covered. The investigator should maintain a singleness of purpose during the interview and should resist any efforts to shorten the interview or drift from topics of concern.

Developing Rapport

The investigator should have a comfortable style that projects professionalism and competence and should generate rapport with the person being interviewed. An open approach that conveys a willingness to communicate generally fosters rapport. Rapport is evident when the individual appears comfortable with the investigator and is willing to confide personally sensitive information. Continuing rapport can oftentimes be maintained if the investigator does not become judgmental when disagreeable conduct or information is disclosed. The investigator who can project empathy when appropriate to do so often gains special insight but, at the same time, no investigator should get personally involved with the case.

Handling Hostility

If the investigator feels threatened by the individual being interviewed, the investigator should stop the interview and report the situation to the appropriate authorities.

Investigators may encounter argumentative individuals. When this type of hostility is encountered, the investigator can seek to defuse it by explaining the purpose of the interview and that the interview is a required part of the investigation. Reminding the interviewee that the investigator has full authority to conduct the interview and that the interviewee is required to cooperate may lessen the reluctance. **[See, however, the discussion above regarding warnings that must be given when requiring the subject of an investigation to cooperate.]**

Recognizing and acknowledging the person's hostility and the reason for it will sometimes let both parties reach the mutual understanding that the interview will proceed (whether or not the topics under discussion are related to the hostility).

If, after repeated attempts in various ways, an individual refuses to answer a specific question, the investigator should attempt to learn the reason. The manager should record the refusal to answer any question and the reason. If the individual wants to terminate the interview, the

manager should attempt to learn the reason and to dissuade the individual by addressing the concerns. If the individual persists, the manager should conclude the interview.

ADMINISTRATIVE AND DISCIPLINARY CONSIDERATIONS

I.   OVERVIEW

Having an understanding of the issues that come into play in violent and potentially violent situations is important for all members of an agency's planning group. It helps in coordinating an effective response, in determining whether outside resources will be needed in certain situations, and in ensuring that appropriate disciplinary actions are taken.

In some agencies, the HR staff coordinates the workplace violence program. One reason is most reported incidents will result in some type of disciplinary action. Another reason is, since the goal of the workplace violence prevention effort is to deal effectively with problem behavior early on, reporting incidents to HR can result in swift disciplinary action which will stop the unacceptable behavior before it can escalate. When another office, such as the Security Office, is responsible for coordinating the response effort, immediate involvement of HR is usually necessary for an effective response.

This section will discuss:

- Administrative options available in removing potentially dangerous employees from the work site;
- Taking appropriate disciplinary action based on violent, threatening, harassing, and other disruptive behavior;
- Responding to an employee who raises a medical condition/disability as a defense against the misconduct;
- Offering EAP Services; and
- Information on appeals of disciplinary actions.

II.   ADMINISTRATIVE ACTIONS TO KEEP AN EMPLOYEE AWAY FROM THE WORK SITE

In situations where a disruption has occurred on the job, or where there is a belief that the potential for violence exists, a supervisor may need to keep an employee away from the work site to ensure the safety of employees while conducting further investigation and deciding on a course of action. When choosing any of these options, be sure you are in compliance with due process and problem solving procedures.

Immediate, Short-term Actions

Place Employee On Administrative Leave. Placing the employee on a paid, non-duty status is an immediate, temporary short-term solution to the problem of an employee who should be kept away from the work site. Some employees who are placed on administrative leave consider this measure to be punitive. However, relevant statute and case law have indicated that as long as the

employee continues receiving pay and benefits just as if he or she were in a duty status, placing the employee on an administrative leave status does not require the use of adverse, action procedures. Agencies should monitor the situation and move toward longer-term actions (as discussed below) when it is necessary, appropriate, or prudent to do so. Depending on the circumstances, it may also be a good idea to offer the employee the option to work at home while on administrative leave.

Reassign Employee To Another Position. This can be an effective way of getting an employee away from the work site where he or she is causing other employees at the work site to be disturbed. However, this action will be useful only if there is another position where the employee can work safely and without disrupting other workers.

Longer-term Actions

Supervisors are sometimes faced with a situation where there is insufficient information available to determine if an employee poses a safety risk, has actually committed a crime, or has a medical condition, which might make disciplinary action inappropriate.

Suspension For Investigation. A suspension for investigation is an action that takes an employee off-duty until the completion of an ongoing inquiry, such as an agency investigation into allegations of misconduct. A letter must be provided to the employee stating that the employee is being suspended for investigation with pay for up to thirty (30) days, which sections of the Division of Human Resource Rules are subject of the investigation, and the effective date of the suspension. Agencies usually propose suspensions for investigations when they will need more than a few days to await the results of an investigation, await the completion of a criminal proceeding, or make a determination on the employee's medical condition. The suspension may be extended, if necessary.

III.   DISCIPLINARY ACTION

Once all the relevant information is obtained, the appropriate appointing authority, HR representative and, if appropriate, the Deputy Attorney General, must determine the appropriate disciplinary action. Some disciplinary actions are:

- **Verbal warning** – Properly recorded and clearly documenting the discussion with the employee and items discussed, such as the issue at hand, what actions or behaviors are not acceptable, future behavior expectations and consequence of future occurrences.
- **Written Reprimand** – A letter to the employee clearly documenting the discussion with the employee and items discussed, such as the issue at hand, what actions or behaviors are not acceptable, future behavior expectations and consequence of future occurrences. This letter should be signed by the employee indicating receipt and understanding of the contents and a signed copy placed in the employee's personnel file.

These lesser disciplinary actions can be used in cases where the misconduct is not serious and progressive discipline may correct the problem behavior. They can be an excellent means of dealing with problem behavior early on.

If the action is more severe, other levels of discipline that could be considered include:

- **Suspension** – Placing the employee on a period of unpaid leave. This is an adverse action and requires "Due Process" in accordance with Idaho Code and the Division of Human Resource Rules. The employee must be provided a letter notifying him/ her of the contemplated suspension, the basis for the proposed action and providing the employee the opportunity to respond.
- **Dismissal** – Again, this is an adverse action and requires "Due Process" in accordance with Idaho Code and the Division of Human Resource Rules.

IV. DISABILITIES AS A DEFENSE AGAINST ALLEGED MISCONDUCT

The Equal Employment Opportunity Commission (EEOC) has issued important guidance that specifically addresses potentially violent misconduct by employees with disabilities. Although this guidance deals specifically with psychiatric disabilities, it applies generally to other disabling medical conditions. It advises that an agency may discipline an employee with a disability who has violated a rule (written or unwritten) that is job-related and consistent with business necessity, even if the misconduct is the result of the disability, as long as the agency would impose the same discipline on an employee without a disability. The guidance specifically states that nothing in the Rehabilitation Act prevents an employer from maintaining a workplace free of violence or threats of violence.

The guidance specifically states that reasonable accommodation is always prospective. Thus, an agency is never required to excuse past misconduct as a reasonable accommodation. A reasonable accommodation is a change to the workplace that helps an employee perform his or her job and may be required, along with discipline, when the discipline is less than removal.

- **Action procedures.** Agencies should monitor the situation and move toward longer-term actions (as discussed below) when it is necessary, appropriate, or prudent to do so. Depending on the circumstances, it may also be a good idea to offer the employee the option to work at home while on administrative leave.
- **Reassign employee to another position.** This can be an effective way of getting an employee away from the work site where he or she is causing other employees at the work site to be disturbed. However, this action will be useful only if there is another position where the employee can work safely and without disrupting other workers.

EMPLOYEE ASSISTANCE PROGRAM CONSIDERATIONS

I.   OVERVIEW OF THE EMPLOYEE ASSISTANCE PROGRAM (EAP)

Every agency has access to an EAP (under contract), which provides short-term counseling and referral services to its employees at no cost. Professional counselors are available to discuss problems that can adversely affect job performance, conduct, and reliability staff these programs. EAPs are required to help employees deal with alcoholism or drug abuse problems, and most programs also help employees with other problems, such as marital or financial problems. EAP counselors often refer employees to other professional services and resources within the community for further information, assistance, or long-term counseling.

Confidentiality is an important issue for EAPs. Employees who seek EAP services are afforded considerable privacy by laws, policies, and the professional ethics of EAP professionals. It is common practice for EAPs to inform employees in writing about the limits of confidentiality on their first visit.

Agency planning group members should familiarize themselves with the structure, scope, and special considerations of the EAP. As the planning group explores the range of services provided, it may identify needs for expanding the program's existing array of services. EAP professionals should advise the agency-planning group on the relevant laws, policies, and professional ethical constraints under which they operate, including any applicable statutory provisions affecting privacy.

II.   INTRODUCTION

EAP participation can be important to the success of an agency's workplace violence program. The EAP's role generally begins with participation on the agency planning group where decisions are made about the role the EAP will play in the workplace violence program. EAPs usually play an active role in early prevention efforts, sometimes participate on the IRT, and generally assist with organizational recovery after an incident of workplace violence has occurred. This section will provide an overview of the EAP and then discuss considerations specific to workplace violence.

III.   THE EMPLOYEE ASSISTANCE PROGRAM'S ROLE IN DEALING WITH WORKPLACE VIOLENCE

EAP staff members generally assist in policy and strategy development and help determine the EAP's role on the agency's workplace violence IRT. EAP counselors bring a special expertise to the planning process. They are in an optimal position to assist with many of the activities conducted by the planning group.

Role In Early Prevention Efforts

Promotion Of The EAP. The effectiveness of a workplace violence program is greatly enhanced in an organization with an active, well-known EAP presence. Agencies with active programs promote the EAP by issuing periodic statements from top management endorsing the program and reminding employees of the services offered by the EAP, having counselors attend staff meetings to familiarize agency employees with the counselors, and having counselors give special briefings and seminars for managers and employees.

Information Dissemination. EAP's often provide booklets, pamphlets, and lending libraries of books and videos about such topics as domestic violence, stress reduction, and dealing with angry customers.

Early Involvement In Organizational Change. When an agency is facing reorganization, restructuring, or any other organizational changes that may have a negative effect on employees, the EAP can help. They can provide individual or group sessions, keep information flowing, keep feelings under control, prevent potential outbursts, provide constructive outlets for feelings, and help employees plan for the future.

Employee And Supervisory Training. The EAP provider may be a resource to provide training on such topics as dealing with angry coworkers and customers, conflict resolution, and communications skills. Since EAP providers understand how important it is that supervisors (and coworkers) not diagnose an employee's problem, they are in an excellent position to explain the delicate balance between identifying problem behavior early on and labeling an individual as potentially violent. EAP counselors may provide insight and assistance to supervisors in dealing with problems as soon as they surface without diagnosing the employee's problem.

Participation On An IRT

Since every reported incident of workplace violence is different and every agency is structured differently, EAP participation on an IRT will depend on many factors. Issues need to be clarified ahead of time to avoid misunderstanding and conflict. Team members need to understand that, due to confidentiality issues, if a case is being discussed and the counselor says, *Sorry, I can't help you with this one,* they should neither expect an explanation nor assume that the counselor is being uncooperative. Advance planning can help to identify ways of coping with these types of issues. For example, if the EAP is large enough, different staff members may play different roles, or the staff may be able to identify other professionals who can be brought in to ensure that all needs are addressed. Working with other members of the planning group and the IRT in advance can clarify the EAP's role when an incident arises.

Consultation With Supervisor When Incident Is Reported. Depending on the type of incident reported, it is often important for a counselor, along with an HR specialist and security officer, to be part of the IRT that consults with the manager. In some situations, such as potential suicides, the EAP can play a major role. In other situations, such as dealing with an employee

who frightens coworkers but who has not actually done or said anything warranting discipline, the EAP can assist other team members in working with the supervisor to plan an effective response.

Response/Intervention. The EAP counselor can help with conflict resolution in situations that are reported early enough for such an intervention. The counselor can work with the victim, giving advice and guidance, or with the perpetrator, helping to diffuse the anger/hostility that could lead to violence. The counselor can help clarify options and procedures for situations in which substance abuse or mental illness seems to be a factor. For example, states differ in their laws regarding civil commitment for psychiatric treatment. The counselor can explain to other team members the EAP role in such a situation and can coordinate with other community resources to develop contingency plans for various emergency situations.

Follow-up To A Violent Incident

Many EAP counselors are prepared to respond promptly to a variety of needs that may exist after a violent incident. Prompt individual interventions with employees who have had particularly stressful experiences are sometimes necessary. Debriefing sessions for groups are often conducted two or three days after the incident. The EAP can also act as a consultant to management in helping the organization to recover.

Individual Interventions. Though most employees will need only brief intervention, provision should be made for the few who may need longer-term professional assistance. Strategies for identifying these employees and guiding them as smoothly as possible from emergency-centered interventions to more extensive mental health care should be included in the planning.

The EAP may approach these responsibilities in different ways, depending on the size and experience of its staff. In some cases, internal EAP resources may be sufficient, but in others, additional staffing will be necessary. EAP staff who do not have expertise in traumatic incident counseling may wish to develop in-house expertise or keep close at hand the phone numbers of resources to contact should an incident occur. Potential sources of additional help, for example, private contractors, community mental health resources, university or medical school programs, might be explored.

Acting As Consultants To Management. Since management bears the brunt of responsibility after a violent incident and can find itself dealing with unfamiliar challenges under high stress, the EAP can be very helpful in facilitating an optimal response. It can provide managers with information on traumatic events and can assist them in analyzing the situation and developing strategies for the organization's recovery. An effective EAP needs to be familiar not only with post-disaster mental health care, but also with management practices that facilitate recovery, and with other resources, which may need to be mobilized.

In thinking about an organization's recovery, there is a temptation to focus narrowly on care-giving responses, such as debriefings and counseling discussed above. Essential as these services are, they are only part of the picture. The way the manager conveys information, schedules

responsibilities, sets priorities, and monitors employee performance after a violent incident can play a vital role in helping or hindering recovery. Some EAP counselors are trained to provide this type of consultation.

IV.   OTHER EAP CONSIDERATIONS FOR THE AGENCY IRT

Should The EAP Take The Incident Report?

Most agencies do not use the EAP as the office responsible for taking incident reports on workplace violence. Agencies give the following reasons: because confidentiality requirements prohibit EAP counselors from disclosing information and putting a counselor in the position of informing the other members of the IRT about the report could lead to serious misunderstandings among agency employees, this could harm the credibility of the EAP. It sometimes takes years to build the EAP into a viable program trusted by employees to keep any contacts confidential, and the dual role could diminish this viability.

Many times the EAP counselor will be the person who first hears about an incident involving threatening behavior, even though the agency's reporting system provides for another office to take incident reports. Managers and employees often feel comfortable telling the counselor about a situation that frightens them. The agency's planning group should decide ahead of time which types of reports the counselors should handle alone and which types should be reported to the other team members, always making sure that each member of the team understands the confidentiality requirements of the EAP.

Should The EAP Be The First Intervenor?

Agencies who have had experience with the EAP counselor being the first intervenor in workplace violence situations report that they do not recommend this approach for the following reasons:

- Issues of confidentiality cause numerous conflicts for the counselors, and
- A perception of treating perpetrators of workplace violence as victims needing counseling rather than as perpetrators needing discipline could be created.

Therefore, the agency-planning group should ensure that procedures developed in advance allow for flexibility and do not require counselors to be the first intervenors in situations where this would be inappropriate

Should The EAP Perform Psychological Exams?

Organizations with experience in **offering** psychological or psychiatric examinations usually recommend that the EAP staff **not** perform these. The process of conducting these examinations is not only time-consuming and highly specialized, but it also fits poorly with other EAP responsibilities. Thus, most agencies find it preferable, if offering such an examination, to have it

done by an "outsider", such as an external contractor. The State of Idaho EAP provider services are contracted and considered an external contractor. The EAP can then take the role of teacher and facilitator, helping everyone involved to understand the report of the examination and put its recommendations into practice.

WORKPLACE SECURITY

I. OVERVIEW

This section will cover:

- Security planning;
- Law enforcement and security assistance; and
- Physical security measures.

II. INTRODUCTION

Law enforcement and security officers should be involved in all stages of the planning process in an effective workplace violence prevention program. They can play an active role in prevention, intervention, and response to threatening situations, in addition to their traditional role of responding to actual incidents of physical violence. This section will provide general ideas and considerations that can help the agency planning group gain an understanding of some of the law enforcement and security issues, such as jurisdiction. It is also intended to help those state agencies and offices that do not have in-house security or law enforcement identify the appropriate organizations that can assist them.

III. SECURITY PLANNING

Depending on the agency, location of the office, and the type of incident or situation, jurisdiction may vary. The State's own law enforcement organization, the Department of Law Enforcement, or Federal, or local law enforcement, or a combination of these, may have jurisdiction. There also may be gaps in law enforcement coverage when issues of workplace violence arise. These gaps can be closed if the agency planning group (which would include any in-house security organization) works with the various law enforcement organizations in setting up workplace violence programs. The following are some suggestions for involving law enforcement in agency efforts to prevent workplace violence.

Jurisdiction

The agency planning group should identify which law enforcement agency or agencies have responsibility for its work site. For example, the primary law enforcement service for responding to incidents in the Capitol Mall, under the charge and control of the Department of Administration as an owned or leased facility, would be either the Idaho State Police or Boise City Police – depending on the type and location of the incident. Some agencies have in-house security and/or law enforcement organizations. Others have contracts with private security firms. It is not always clear who has jurisdiction, and who should be contacted when the need arises.

Sometimes meeting with the local police chief, county sheriff, or state police is necessary to establish a plan or procedure regarding law enforcement response in the event of potential violence or hostile incidents. Sometimes new building agreements will be necessary or contracts will have to be modified. In remote locations, arrangements can be made for local police to handle emergency situations and to work with the appropriate State Police officials. The State Security Manager can assist with many of these issues and can respond to any location.

Liaison With Law Enforcement Agencies

The agency planning group, and later the IRT, should maintain open and continuous liaison with those law enforcement agencies responsible for their work site. This would entail having periodic meetings to discuss the agency's concerns. Without these contacts, lines of communication can break down and misunderstandings could arise. It is during these contacts that the agency can obtain the names and telephone numbers of law enforcement personnel to be called upon should the need arise. Planning groups in agencies that already have established liaisons should work through these established liaisons to avoid confusion.

IV. LAW ENFORCEMENT AND SECURITY ASSISTANCE

During the planning phase, law enforcement/security officers can:

- Identify types of situations they can address and when and how they should be notified of an incident;
- Indicate whether their officers have arrest authority;
- Identify their jurisdictional restrictions and alternative law enforcement agencies that may be able to provide assistance;
- Identify threat assessment professionals who can assist the agency in its efforts to protect threatened employees;
- Advise on what evidence is necessary and how it can be collected or recorded, so that law enforcement can assess the information and decide what action to take, if appropriate;
- Explain anti-stalking laws applicable in the agency's jurisdiction and how and when to obtain restraining orders;
- Suggest security measures to be taken for specific situations, such as in cases where EAP counselors or other mental health professionals warn the agency that an individual has made a threat against an agency employee; and
- Arrange for supervisor and employee briefings or training on specific workplace violence issues such as:
  - Personal safety and security measures;
  - Types of incidents to report to law enforcement/security;
  - Types of measures law enforcement/security may take to protect employees during a violent incident, i.e., explanations of what it means to "secure the area", "secure the perimeter", and "preserve evidence";
  - Suggestions on how to react to an armed attacker; and

- • Suggestions for dealing with angry customers and clients, suspicious packages, bomb threats, hostage situations, and telephone harassment and threats.

When potentially violent situations arise, law enforcement and security officers can work with the IRT to:

- • Provide an assessment of the information available to determine whether law enforcement intervention is immediately necessary. For example, whether a criminal investigation is appropriate and whether a threat assessment professional should be consulted;
- • Identify what plan of action they deem appropriate; and
- • Determine who will gather what types of evidence.

V.   PHYSICAL SECURITY MEASURES

Many state agencies have numerous security measures in place that can reduce the risk of workplace violence. These include closed circuit cameras, silent alarms, two-way mirrors, electronic access systems, barriers to prevent cars from driving too close to the building, emergency internal code words, extra lighting in the parking lots, and escorts to and from parking lots after dark. Planning groups should review security measures and procedures and make recommendations for modifications and improvements as necessary.

The following are some suggestions provided by the State Security Manager on methods to improve security in your office and/or building.

- • Post a security officer at the main building entrance or at entrances to specific offices;
- • Install a metal detector or closed-circuit television (CCTV) camera or other device to monitor people coming in all building entrances;
- • Make sure your employees have photo identification cards and assign temporary passes to visitors, who should be required to sign in and out of the building. Under certain conditions, security officers should be required to call offices to confirm an appointment and/or to request an escort for all visitors -- customers, relatives, or friends;
- • Brief employees on steps to take if a threatening or violent incident occurs;
- • Establish code words to alert coworkers and supervisors that immediate help is needed; and
- • Install silent, concealed alarms at reception desks.

The following are some recommendations provided by the State Security Manager's Office of ways to improve security in "front-line" offices that serve the public.

- • Ensure that security officers have a clear view of the customer service area at all times;
- • Arrange office furniture and partitions so "natural" barriers (desks, countertops, and partitions) surround those front-line employees in daily contact with the public to separate employees from customers and visitors;

- Provide an under-the-counter duress alarm system to signal a supervisor or security officer if a customer becomes threatening or violent;
- Establish an area in the office for employees and/or customers to escape to if they are confronted with violent or threatening people;
- Provide an access-control combination lock on access doors; and
- Mount closed circuit television cameras for monitoring customer service activity from a central security office for the building.

ORGANIZATIONAL RECOVERY AFTER AN INCIDENT

I. OVERVIEW

This section will cover:

- Management presence and responsibility;
- Sharing information with employees;
- Working with crisis response professionals;
- Support for the debriefing process;
- Support for care giving within the work groups;
- Handling critical sites with care;
- Buffering those affected from post-event stresses; and
- Helping employees return to the work site.

II. INTRODUCTION

Despite the best-laid plans of any agency, violence in the workplace can happen. Just as agencies develop policies and procedures designed to head off these occurrences, agencies must be equally prepared to deal with the aftermath of such incidents. Quite often management's focus will be on getting the operational side of the office back in working order. However, just as important as getting the office back on-line is attending to the impact such incidents can have on office personnel. This section will provide information designed to assist management with helping an organization to recover after an incident of workplace violence. Listed below are several initial steps management can take when an incident of workplace violence occurs.

Ensure A Management Presence In The Work Site

Managers need to spend ample time with their employees at the work site or wherever they may be. Employees need to be reassured of management's concern and they need to be able to ask questions. Senior management should ensure that immediate supervisors are supported in this role, relieved of unnecessary duties, and not pulled away from their subordinates to write lengthy reports or prepare elaborate briefings.

Share Information With Employees

Employees will have many questions, and they need the answers (avoiding any potential breach of confidentiality), often more than once, if they are to resolve the experience for themselves. Information will develop over time, so information strategies need to be simple and fluid. A notice board at the elevator, or a recorded message on a "hotline" number may suffice for the basics, and a user-friendly system for individual questions needs to be established.

Bring In Crisis Response Professionals

Before an incident ever occurs, the planning group should identify trained mental health professionals in the agency's EAP or the community who would be available to respond in the event of an incident. When an incident occurs, involve these emergency mental health consultants as soon as possible. They will generally meet with management first, working down the chain, and then with line employees. Based on what the consultants learn, they will offer services such as debriefing techniques and informal counseling, perhaps in the work area.

Support Informal Debriefing

The formal debriefing doesn't end the recovery process. Provide opportunities for employees to talk informally with one another when they feel a need to discuss the experience. A comfortable break area and flexibility about break times may be all that is needed.

Support Care Giving Within Work Groups

Keep work groups together as much as possible, and try not to isolate employees from their normal support groups at work. Show respect and support for employees' efforts to care for one another.

Handle Critical Sites With Care

Initially, the site of a violent incident will be secured as a crime scene. After the authorities are finished with it, management needs to be sensitive to a number of issues. It is helpful if employees don't have to come back to work and face painful reminders, such as bloodstains or broken furniture. But on the other hand, the area should not be so "sanitized" that it gives the appearance that management is pretending nothing happened. If someone has died, that person's work area will be a focus of grieving, and it needs to be respected as such.

Buffer Those Affected From Post-Event Stresses

Effective coordination with the media and timely dissemination of information can help reduce media pressure on those who are the most vulnerable. Assistance with benefits and other administrative issues can reduce the burden on victims and families.

Help Employees Face Feared Places Or Activities

Returning soon, if only briefly, to a feared site can help prevent lasting effects, such as phobic responses. Having a friend or loved one along or being supported by close work associates may make the first step much easier.

Remember The Healing Value Of Work

Getting back to work can be reassuring, and a sense of having a mission to perform can help the group recover its morale. But the return to work must be managed in a way that conveys appropriate respect for the deceased, the injured, and the traumatized.

ABBREVIATIONS

ADR   Alternative Dispute Resolution

CCTV   Closed-circuit Television

EAP   Employee Assistance Program

EEOC   Equal Employment Opportunity Commission

HR   Human Resources

IRT   Incident Response Team

RIF   Reduction in Force

EXAMPLES OF USEFUL HANDOUTS FOR EMPLOYEES

The attached desk card summarizes the actions you should (or should not) take in a hostile or threatening situation. Print out and detach the card, tear or cut along the dotted lines, fold the card into a "tent", and tape the ends together underneath so that the card will stand up on your desk with the text facing you. Review the card often. That way, if an angry, hostile, or threatening customer or coworker confronts you, you will know what you should do. Everyone in your office, including supervisors and managers, should follow these same procedures. You can make copies of this card so that everyone has his or her own card.

Coping With Threats and Violence
- For an angry or hostile customer or coworker
    - Stay calm. Listen attentively.
    - Maintain eye contact.
    - Be courteous. Be patient.
    - Keep the situation in your control.

For a person shouting, swearing, and threatening
- Signal a coworker, or supervisor, that you need help. (Use a duress alarm system or prearranged code words.)
- Do not make any calls yourself.
- Have someone call the Security Office, or local police.

For someone threatening you with a gun, knife, or other weapon
- Stay calm. Quietly signal for help. (Use a duress alarm or code words.)
- Maintain eye contact.
- Stall for time.
- Keep talking -- but follow instructions from the person who has the weapon.
- Don't risk harm to yourself or others.
- Never try to grab a weapon.
- Watch for a safe chance to escape to a safe area.

Telephone Threats
- Keep calm. Keep talking.
- Don't hang up.
- Signal a coworker to get on an extension.
- Ask the caller to repeat the message and write it down.
- Repeat questions, if necessary.
- **For a bomb threat**, ask where the bomb is and when it is set to go off.
- Listen for background noises and write down a description.
- Write down whether it's a man or a woman; pitch of voice, accent; anything else you hear.
- Try to get the person's name, exact location, and telephone number.
- Signal a coworker to immediately call the Security Office, a security officer, or the local police.
- Notify your immediate supervisor.

PREVENTING WORKPLACE VIOLENCE – DESK CARD

Preventing Workplace Violence – Desk Card

Coping With Threats and Violence	*For A Person Shouting, Swearing, And Threatening*

• For an angry or hostile customer or coworker
   ▪ Stay calm. Listen attentively.
   ▪ Maintain eye contact.
   ▪ Be courteous. Be patient.
   ▪ Keep the situation in your control.
	• Signal a coworker, or supervisor, that you need help. (Use a duress alarm system or prearranged code words.)
	• Do not make any calls yourself.
	• Have someone call the Security Office, or local police.

For Someone Threatening You With A Gun, Knife, Or Other Weapon • Stay calm. Quietly signal for help. (Use a duress alarm or code words.) • Maintain eye contact. • Stall for time. • Keep talking -- but follow instructions from the person who has the weapon. • Don't risk harm to yourself or others. • Never try to grab a weapon. • Watch for a safe chance to escape to a safe area.	*Telephone Threats* • Keep calm. Keep talking. • Don't hang up. • Signal a coworker to get on an extension. • Ask the caller to repeat the message and write it down. • Repeat questions, if necessary. • **For a bomb threat**, ask where the bomb is and when it is set to go off. • Listen for background noises and write down a description. • Write down whether it's a man or a woman; pitch of voice, accent; anything else you hear. • Try to get the person's name, exact location, and telephone number. • Signal a coworker to immediately call the Security Office, a security officer, or the local police. • Notify your immediate supervisor.